

JAN 16 2007

Jenkins & Gilchrist
A PROFESSIONAL CORPORATION225 WEST WASHINGTON
SUITE 2600
CHICAGO, ILLINOIS 60606(312) 425-3900
TELECOPIER (312) 425-3909www.jenkins.com

FROM THE DESK OF:

Wayne L. Tang
(312) 425-8641AUSTIN, TEXAS
DALLAS, TEXAS
HOUSTON, TEXAS
LOS ANGELES, CALIFORNIA
SAN ANTONIO, TEXAS

RECIPIENT

Examiner:
Jasson H. Yoo
ART UNIT: 3714

COMPANY

U.S. Patent & Trademark
Office

FAX NO.

(571) 273-8300

PHONE NO.

• MESSAGE •

SERIAL NO. 10/630,036 – John J. Giobbi**NOTICE OF CONFIDENTIALITY**

The information contained in and transmitted with this facsimile is

1. SUBJECT TO THE ATTORNEY-CLIENT PRIVILEGE;
2. ATTORNEY WORK PRODUCT; OR
3. CONFIDENTIAL.

It is intended only for the individual or entity designated above. You are hereby notified that any dissemination, distribution, copying, or use of or reliance upon the information contained in and transmitted with this facsimile by or to anyone other than the recipient designated above by the sender is *unauthorized and strictly prohibited*. If you have received this facsimile in error, please notify Jenkins & Gilchrist, a professional corporation, by telephone at (312) 425-3900 immediately. Any facsimile erroneously transmitted to you should be immediately returned to the sender by U.S. Mail, or if authorization is granted by the sender, destroyed.

Time: 10:41am Date: Jan 16, 2007

Emp. #: 5427

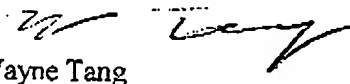
Billing #: 47079-
107USD1

Total Pages (7):

CHICAGO 344733v1 99999-00001

Dear Examiner Yoo:

As per our discussion today, I am enclosing a proposed amendment to differentiate the encoding methods of the cited references and the encryption that the present claims perform. I am attaching a definition from PCMag.com which provides a technically understood meaning of cryptography which the proposed claim amendment is derived from. Unlike encoding which simply substitutes text in a predetermined pattern, encryption combines the key bits with the data bits to create ciphertext. As I mentioned, we would like to see if such an amendment may help to allow this case and would like the opportunity for either a formal or informal interview if you believe that it would help with allowing the case.



Wayne Tang

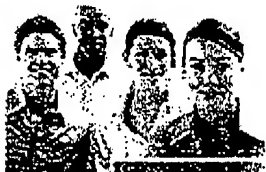
Reg. No. 36,028



DIGITAL CAMERAS LAPTOPS MP3 PLAYERS CELL PHONES PRINTERS DESKTOPS HDTVS

PCMAG.COM
THE INDEPENDENT GUIDE TO TECHNOLOGY

Sign In | Reg



Online Meetings Can Save You Time

GoToMeeti
TRY IT
FREE
CLICK HERE

HOME	REVIEWS	DOWNLOADS	EXPERT HELP	NEWS	COLUMNS	SHOP	DISCUSS	@WORK
Ask Loyd	Ask Neil	DIY	Travel	Vista Revealed	Security Watch Newsletter	Security Watch	SMB Boot	
Software	Hardware	Tips	Encyclopedia					

SEARCH ☒ PCMAG.COM ☐ EXPERT HELP

SEARCH

PC Magazine:
Current Issue

Previous Issues

[Home](#) > [Expert Help](#) > [Encyclopedia](#) > cryptography

AD:



Search:

Search Encyclopedia

[Browse the Index](#)

Definition of: cryptography

The conversion of data into a secret code for transmission over a public network. The original text, or "plaintext," is converted into a coded equivalent called "ciphertext" via an encryption algorithm. The ciphertext is decoded (decrypted) at the receiving end and turned back into plaintext.

Keys Are the Key

The encryption algorithm uses a "key," which is a binary number that is typically from 40 to 256 bits in length. The greater the number of bits in the key (cipher strength), the more possible key combinations and the longer it would take to break the code. The data are encrypted, or "locked," by combining the bits in the key mathematically with the data bits. At the receiving end, the key is used to "unlock" the code and restore the original data.

Secret Vs. Public Key

Secret key cryptography and public key cryptography are the two major cryptographic architectures.

Secret Keys - Symmetric System

The first method uses a secret key, such as the DES and AES algorithms. Both sender and receiver use the same key to encrypt and decrypt. This is the fastest computation method, but getting the secret key to the recipient in the first place is a problem that is often handled by the second method.

Public Keys - Asymmetric System

The second method uses a two-part key, such as RSA and El Gamal. Each recipient has a private key that is kept secret and a public key that is published for everyone. The sender

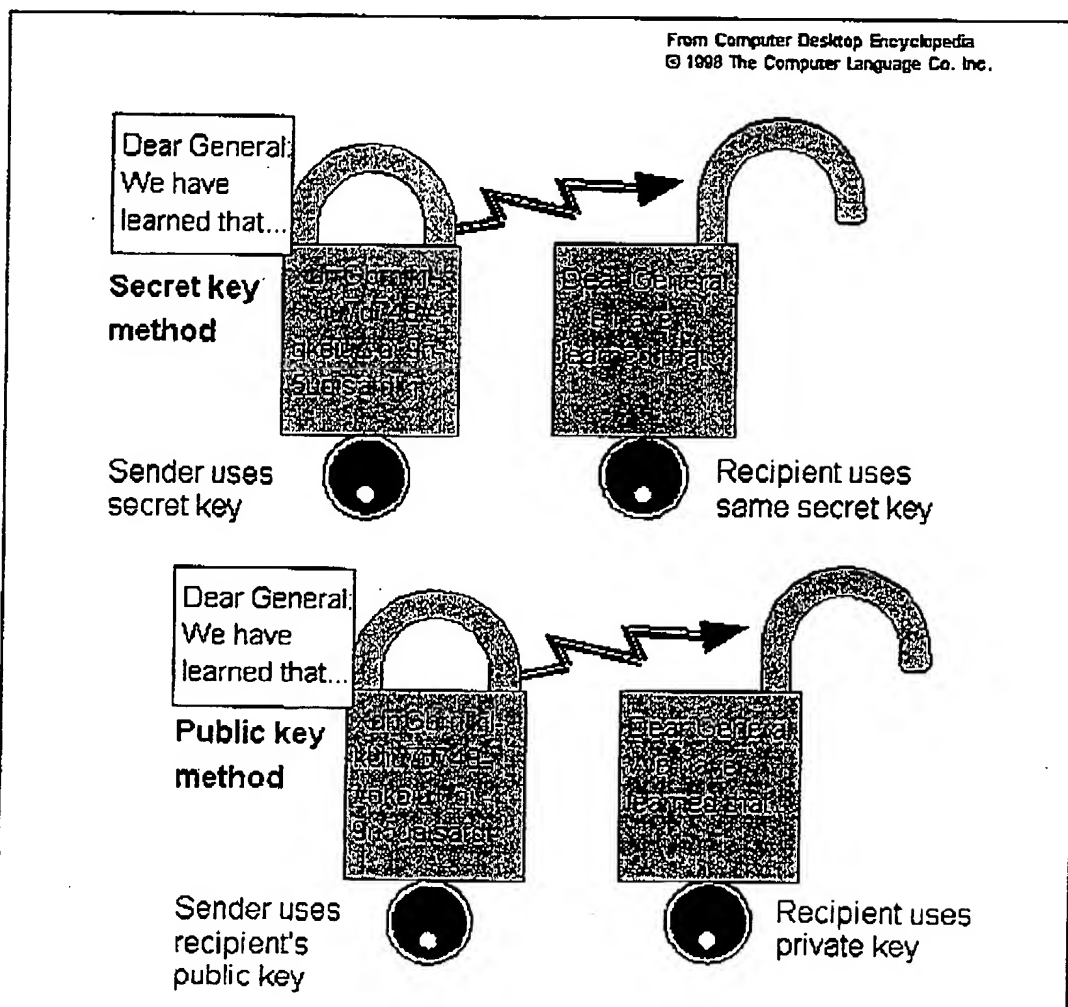
looks up or is sent the recipient's public key and uses it to encrypt the message. The recipient uses the private key to decrypt the message and never publishes or transmits the private key to anyone. Thus, the private key is never in transit and remains invulnerable.

Both Are Used Together

Secret key and public key systems are often used together, such as the AES secret key and the RSA public key. The secret key method provides the fastest decryption, and the public key method provides a convenient way to transmit the secret key. This is called a "digital envelope." For example, the PGP e-mail encryption program uses one of several public key methods to send the secret key along with the message that has been encrypted with that secret key (see [PGP](#)).

Get Faster - Get Stronger

It has been said that any encryption code can be broken given enough time to compute all permutations. However, if it takes months to break a code, the war could already be lost, or the thief could have long absconded with the money from the forged financial transaction. As computers get faster, to stay ahead of the game, encryption algorithms have to become stronger by using longer keys and more clever techniques. See [XOR](#), [AES](#), [DES](#), [RSA](#), [plaintext](#), [digital signature](#), [digital certificate](#), [steganography](#) and [chaff](#) and [winnow](#).



ava
dec
5th!

PARTNE

Enter to
MacBoc

2 Free 1
from 1B

Search
quality.
Dice.co

Is your
Visit Sn
Central

RELATEI

RSA En
Public I

Secret Key Vs. Public Key

The secret method uses the same key to encrypt and decrypt. The problem is transmitting the key to the recipient in order to use it. The public key method uses two keys: one kept private and never transmitted, while the other is made public. Very often, the public key method is used to safely send the secret key to the recipient so that the message can be encrypted using the faster secret key algorithm.

RSA Ke

Secret I
Cryptos

Code Cr

World
Stora
AppliOn the
with JTop 4
SpecPlot Y
the E
Grid

to list y

Some Public History About Secret Methods

The following is reprinted with permission from RSA Security, Inc.

In 1518, a Benedictine monk named Johannes Trithemius wrote "Polygraphiae," the first published treatise on cryptography. Later, his text "Steganographia" described a cipher in which each letter is represented by words in successive columns of text, designed to hide inconspicuously inside a seemingly pious book of prayer.

Polygraphiae and Steganographia attracted a considerable amount of attention not only for their meticulous analysis of ciphers but more notable for the unexpected thesis of Steganographia's third and final section, which claimed that messages communicated secretly were aided in their transmission by a host of summoned spirits.

As might be expected, Trithemius' works were widely renounced as having magical content - by no means an unfamiliar theme in cryptographic history - and a century later fell victim to the zealous flames of the Inquisition during which they were banned as heretical sorcery.

RELATED TERMS:

[AES](#)
[chaff and winnow](#)
[DES](#)
[digital certificate](#)
[digital signature](#)
[PGP](#)
[plaintext](#)
[RSA](#)
[steganography](#)
[XOR](#)

Search:

Search Encyclopedia

Browse the index



Copyright © 1981- 2006

The Computer Language Company Inc. All other reproduction is strictly prohibited without permission from the publisher.
 All rights reserved.

THIS COPYRIGHTED DEFINITION IS FOR PERSONAL USE ONLY.

ADVERTISEMENT

marketplace

Ads By Google

AES400 Encryption

truExchange Data Secure helps you secure, encrypt, and transport data
www.nubridges.com/solutions/

Encrypted Email - PostX

Simple, secure, no software! See how easy it is to use. Demo